

CLAIMS1  
2

3 I claim:

1        1. A method of securely conveying a data product, the method comprising the steps  
2        of:3            establishing an authorization key that defines (i) verification information indicative of at  
4            least one authorized entity and (ii) a cryptographic key to the data product;  
5            encrypting the authorization key, thereby producing an encrypted authorization key that  
6            can be decrypted using a decryption key; and7            providing the encrypted authorization key to a system that (i) has access to the decryption  
8            key and can therefore decrypt the encrypted authorization key and (ii) is programmed to decrypt  
9            the authorization key and to use the verification information to validate use of the data product.10  
1        2. The method of claim 1, further comprising the steps of:

1        receiving the encrypted authorization key;

2        using the decryption key to decrypt the encrypted authorization key, and thereby  
3        uncovering the verification information and the cryptographic key to the data product; and  
4        using the verification information to validate use of the data product.5  
61        3. The method of claim 2, wherein using the verification information to validate use  
2        of the data product comprises comparing at least a portion of the verification information to  
3        predetermined information associated with the system, to determine whether the system is  
4        authorized to use the data product.

5

1       4.     The method of claim 3, wherein the predetermined information associated with  
2     the system comprises a system ID.

3

1       5.     The method of claim 1, wherein providing the encrypted authorization key to the  
2     system comprises sending the encrypted authorization key to the system via a wireless  
3     communications network.

4

1       6.     The method of claim 1, wherein providing the encrypted authorization key to the  
2     system comprises recording the encrypted authorization key on a data storage medium and then  
3     providing the data storage medium to the system.

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1           9.       The method of claim 8, wherein the predetermined information associated with  
2       the data storage medium comprises a data storage medium ID.

3

1           10. The method of claim 1, wherein the data product comprises a database of  
2 geographic information.

3

11. A method of securely conveying data, the method comprising the steps of:

assembling a set of authorization parameters associated with the data;

computing a first checksum of the set of authorization parameters;

4 generating a first cryptographic key substantially randomly;

5 using the first cryptographic key to symmetrically encrypt the

parameters, so as to produce an encrypted set of authorization parameters;

parameters, so as to produce an encrypted set of authorization parameters;

7 encrypting a combination of the first cryptographic key and the first checksum, so as to

8 produce a header value that can be decrypted using a second cryptographic key; and

providing the header value, together with the data, for access by a receiving end.

ପ୍ରକାଶନ କମିଶନ

12. The method of claim 11, further comprising the following steps performed at the

... in the code, and it's up to us to make sure to decrypt the header value, so as to produce an

卷一  
四  
十一  
三  
一

- 5 retrieving the first cryptographic key and first checksum from the decrypted header value;
- 6 using the first cryptographic key to decrypt the encrypted set of authorization parameters;
- 7 computing a second checksum of the set of authorization parameters;

8               comparing the second checksum with the first checksum, and refusing to access the data  
9       if the second checksum does not match the first checksum; and  
10              using the set of authorization parameters to verify authorization to access the data.

11

1               13.     The method of claim 12, further comprising encrypting the data before providing  
2       the data and header value for access by the receiving end.

3

1               14.     A method of securely conveying data, the method comprising the steps of:  
2       assembling an authorization key that includes verification information indicative of a data  
3       storage medium on which the data is authorized to be stored; and  
4              encrypting the authorization key and the data, thereby producing an encrypted  
5       authorization key and encrypted data;  
6              storing the encrypted authorization key and encrypted data on a given data storage  
7       medium; and

8              thereafter providing the given data storage medium to a system that is programmed to  
9       decrypt the authorization key and to determine, by reference to the verification information  
10      whether the given storage medium is the data storage medium on which the data is authorized to  
11      be stored.

12

1               15.     The method of claim 14, further comprising the system decrypting the encrypted  
2       data only if the verification information indicates that the given storage medium is the data  
3       storage medium on which the date is authorized to be stored.

4

1        16. A method of securely communicating a data product, while allowing the data  
2 product to be used in connection with at least one authorized entity, the at least one authorized  
3 entity having an associated identification code, the method comprising:

4                symmetrically encrypting at least a portion of the data product using a first cryptographic  
5 key, thereby producing an encrypted portion of the data product that can be symmetrically  
6 decrypted using the first cryptographic key;

7                establishing an authorization key including verification information;

8                computing a first value as a first function of input parameters including (i) the  
9 identification code and (ii) a second value;

10               combining the first value with the first cryptographic key to produce a third value;

11               adding the third value to the authorization key;

12               thereafter using the first value as a second cryptographic key to symmetrically encrypt  
13 the authorization key, so as to produce an encrypted authorization key that can be decrypted  
14 using the first value;

15               encrypting at least the second value to produce an encrypted value that can be decrypted  
16 using a third cryptographic key; and

17               providing to a receiving-end at least (i) the encrypted value, (ii) the encrypted  
18 authorization key, and (iii) the encrypted portion of the data product,

19               whereby, if the receiving end has access to the third cryptographic key and the input  
20 parameters, the receiving end may be able to uncover the first authorization key and the  
21 cryptographic key and may therefore be able to access the verification information and decrypt  
22 the encrypted portion of the data product.

23

1        17. The method of claim 16, wherein the data product comprises geographical  
2 information, the authorized entity comprises a navigation system, and the identification code  
3 comprises a navigation system ID.

4

1        18. The method of claim 16, wherein the data product comprises geographical  
2 information, the authorized entity comprises a data storage device, and the identification code  
3 comprises a storage device ID.

4

19. The method of claim 16, wherein the first function comprises a hash function.

二〇一九年卷之三

20. The method of claim 19, wherein the input parameters further include a predetermined segment of the encrypted portion of the data product.

1

21. The method of claim 16, wherein combining the first value with the first cryptographic key to produce a third value comprises computing an XOR sum of the first value and the first cryptographic key.

4

1           22. The method of claim 16, wherein encrypting at least the second value to produce  
2 an encrypted value that can be decrypted with a third cryptographic key comprises:

3

combining the second value with a checksum of the authorization key; and  
using a public key encryption algorithm to encrypt the second value

5

1        23.     The method of claim 16, further comprising the following steps:  
2            receiving at the receiving-end (i) the encrypted value, (ii) the encrypted authorization  
3            key, and (iii) the encrypted portion of the data product,  
4            using the third cryptographic key to decrypt the encrypted value  
5            computing the first value as the first function of the input parameters;  
6            using the first value as the second cryptographic key to symmetrically decrypt the  
7            encrypted authorization key;  
8            extracting the third value from the authorization key;  
9            using the third value and the first value to generate the first cryptographic key; and  
10            using the first cryptographic key to symmetrically decrypt the encrypted portion of the  
11            data product.

12  
1        24.     Th method of claim 23, further comprising, at the receiving-end, verifying the  
2            checksum of the authorization key.

3  
1        25.     The method of claim 23, wherein using the third value and the first value to  
2            generate the first cryptographic key comprises computing an XOR sum of the third value and the  
3            first value.

4  
1        26.     The method of claim 23, further comprising the step of validating use of the data  
2            product by reference to the verification information.

1        27. A method of securing a data product against unauthorized use, while allowing the  
2 data product to be used in connection with at least one authorized entity, the at least one  
3 authorized entity having an associated identification code, the method comprising:

4                symmetrically encrypting at least a portion of the data product using a first cryptographic  
5 key, thereby producing an encrypted portion of the data product that can be symmetrically  
6 decrypted using the first cryptographic key;

7                establishing an authorization key including verification information;

8                computing a first value as a first function of input parameters including (i) the  
9 identification code and (ii) a second value;

10               combining the first value with the first cryptographic key to produce a third value;

11               adding the third value to the authorization key;

12               thereafter using the first value as a second cryptographic key to symmetrically encrypt  
13 the authorization key, so as to produce an encrypted authorization key that can be decrypted  
14 using the first value; and

15               encrypting at least the second value to produce an encrypted value that can be decrypted  
16 using a third cryptographic key.

17  
1        28. The method of claim 27, further comprising randomly generating the first  
2 cryptographic key.

3  
1        29. The method of claim 27, wherein the portion of the data product comprises the  
2 entire database.

30. The method of claim 27, wherein the portion of the data product comprises  
information required to understand contents of the data product.

31. The method of claim 30, wherein the information required to understand contents data product is selected from the group consisting of (i) database decompression and (ii) pointers.

32. The method of claim 27, wherein the data product comprises geographic  
information.

33. The method of claim 27, wherein the data product comprises geographic  
location, the authorized entity comprises a navigation system, and the identification code  
uses a navigation system ID.

34. The method of claim 27, wherein the data product comprises geographic information, the authorized entity comprises a data storage device, and the identification code uses a storage device ID.

35 The method of claim 27, wherein the first function comprises a hash function.

36. The method of claim 27, wherein the input parameters further include a determined segment of the encrypted portion of the data product.

1       37. The method of claim 27, wherein combining the first value with the first  
2 cryptographic key to produce a third value comprises computing an XOR sum of the first value  
3 and the first cryptographic key.

4

1       38. The method of claim 27, wherein encrypting at least the second value to produce  
2 an encrypted value that can be decrypted with a third cryptographic key comprises:  
3             combining the second value with a checksum of the authorization key; and  
4             using a public key encryption algorithm to encrypt the second value

5

1       39. A system for securing a data product against unauthorized use, while allowing the  
2 data product to be used in connection with at least one authorized entity, the system comprising:  
3             a processor;  
4             a data storage medium; and  
5             a set of machine language instructions stored in the data storage medium and executable  
6 by the processor to carry out the method steps of claim 27.